Počítač v ohrožení

10 nebezpečí, která ještě neznáte

Myslíte si, že váš systém je bezpečný? Chyba! Profesionální hackeři přesně vědí, jak se vzdor bezpečnostnímu softwaru nabourat do kteréhokoli počítače. Avšak kdo jejich triky zná, dokáže se před útokem ochránit – a to docela jednoduše.

Text: Valentin Pletzer, *autor@chip.cz*

V TOMTO ČLÁNKU NAJDETE

Nepozorovaně se vetřou do systému, překonají i tu nejlepší ochranu – a pak udeří. Hackeři jsou čím dál tím drzejší, nebezpečnější a stále nacházejí nové cesty, jak váš počítač infikovat škodlivými programy. Kdo se domnívá, že s nejnovějšími aktualizacemi, nejlepším antivirovým programem a nejsilnějším firewallem jsou jeho Windows mimo nebezpečí, bohužel se mýlí. Nové metody hackerů a internetové mafie dokážou otrávit život i bezpečnostním profesionálům. Rizika však lze přinejmenším minimalizovat. Ukážeme vám deset hrozeb, o nichž jste doposud nejspíš ani neslyšeli, a ty nejlepší metody, jak je odvrátit.

1 Bezpečnostní soupravy s bezpečnostními mezerami

Firewall, antivir a antispam – tak zní bezpečnostní doporučení pro každý počítač s Windows. Avšak právě tyto programy představují přímo pozvánku pro internetovou mafii. Stejně jako v každém jiném softwaru i ve firewallech a v antivirových nástrojích se totiž vyskytují programové chyby, které se často dají zneužít, jakmile se jen připojíte k internetu, třeba jen kvůli stažení aktualizací.

Jak pustošivý dopad mohou takové chyby mít, ukazuje příklad firewallu Blackice. V tomto bezpečnostním programu objevili hackeři mezeru, využili ji – a prostřednictvím červa Witty během necelé hodiny nakazili všechny firewally Blackice na celé světě. Škůdce pak v napadených počítačích zničil všechna data.

S problémem se potýkají i velké firmy jako Symantec. Jeden hacker nám dokonce předvedl, jak dokáže využít chybu v „Symantec Antivirus Corporate Edition“. Do údajně tak dobře chráněného počítače se bez námahy vetřel za několik okamžiků.

Protiopatření: V takových případech jsou na tahu výrobci bezpečnostního softwaru – musí co nejrychleji zareagovat a chybu odstranit. V žádném případě byste však neměli deaktivovat on-line aktualizace svého bezpečnostního softwaru. Pak by se totiž mohlo stát, že nebudou odstraněny jiné, možná ještě horší chyby. Zmíněnou hackerem demonstrovanou chybu už Symantec opravil. Avšak jisté je jen jedno: stoprocentní ochrana neexistuje!

2 Nebezpečné tiskárny ve firemních sítích

Hackeři neustále pátrají po nejslabších místech počítačových sítí. Svědomití administrátoři proto zesilují ochranu nejen na serveru a ve firewallu, nýbrž také na mnoha klientských PC. Jednu slabinu však přitom často přehlížejí – tiskárnu. Tiskárna zapojená do sítě totiž vlastně představuje také server. Znamená to, že kdo má v úmyslu škodit, může manipulovat s jejím nastavením, a dokonce kompletně ovládnout operační systém tiskárny. Už před několika lety zveřejnil hacker FX z hackerské skupiny Phenoelit informace a nástroje, prostřednictvím kterých lze zmanipulovat tiskárny od HP.

V letošním roce nám zase jiný hacker ukázal modifikovaný tiskový server, na němž běželo hned několik hackerských nástrojů. Pro hackera je přitom velice praktické, že mu zmanipulovaná tiskárna dodá až do domu citlivá data, jako jsou údaje z účtů, výplatní pásky, a dokonce i přístupová hesla – a to vždy, kdykoli si chce nic netušící oběť tyto informace vytisknout.

Protiopatření: Obrana je vlastně docela jednoduchá. Většinou postačí silná hesla v konfigurační konzoli tiskárny a omezená přístupová práva. Důležitý je však také pohled „za humna“. Které další přístroje jsou ještě přímo připojeny do sítě? Cílem hackerů se totiž mohou stát také webové kamery, směrovače bezdrátových sítí, multimediální přehrávače a další zařízení.

3 USB paměť, která si podmaní každý počítač

Každý bezpečnostní expert ví, že jakmile jednou hacker sedí přímo u počítače, nezmůže už nic ani ta nejlepší ochrana. Veřejně přístupné terminály, jako jsou PC v knihovnách nebo supermarketech, jsou proto v maximální možné míře znepřístupněny. K dispozici jsou pouze klávesnice, myš a monitor. Ale i to samo už může stačit...

Hackerské srdce dokážou rozbušit hned dva zdroje chyb. Za prvé se v každém softwaru, a tedy i ve Windows, vyskytuje řada nedokumentovaných klávesových kombinací. Ty útočníkovi umožňují například ve Windows otevřít dialog „Spustit“. Mnohem nebezpečnější jsou však přetečení bufferu v ovladačích „plug & play“.

Na hackerském veletrhu DefCon v Las Vegas jsme si útok nechali předvést přímo na našem notebooku. Demonstrace trvá jen pár sekund. Hacker do USB našeho počítače zastrčil vlastnoručně zhotovený přístroj, „ledka“ na něm krátce zasvítila – a už se Windows poroučejí s modrou obrazovkou. Kdyby nešlo jen o „proof-of-concept“, tedy důkaz funkčnosti, už by byl v našem notebooku nainstalován trojský kůň.

Protiopatření: Nejefektivnější ochranou je deaktivace nebo odpojení nepoužitých USB portů. To ovšem hackerovi nezabrání například v přechodném odpojení klávesnice. Lepší je proto software jako „DeviceWall“ od Centennial Software, který sleduje USB porty. Jak dobře se ovšem proti takovýmto útokům osvědčí, ukáže až praxe.

4 Perfektní hackerský úkryt na pevném disku

Vysoko v kurzu je mezi hackery také tzv. „slackspace“ neboli nepoužité paměťové místo na pevném disku dané koncepcí souborových systémů. Pokud soubor neobsadí kompletní klastr, zůstanou zbývající bajty volné. Hackeři toto místo využívají tak, že do něj informace přímo zapisují a později zpětně čtou pomocí speciálních nástrojů. Zde uložená data sice nelze přímo spouštět, ale představují skvělou skrýš pro ukradená hesla, protokoly keyloggerů a screenshoty. Zvláště pokud jsou ještě také zašifrovány.

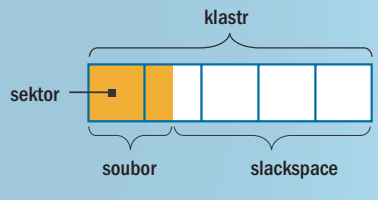
Celou záležitost jsme vyzkoušeli pomocí nástroje „Slacker“ *(www.metasploit.com/projects/antiforensics/)* a diskového editoru. Nejprve do slackspace schováváme nezašifrovaný textový soubor. Pak prostřednictvím diskového editoru přistupujeme přímo na fyzické adresy pevného disku. A hle, tam, kde je oblast slackspace zvláště velká, objevujeme fragmenty našeho souboru. S použitím jiného parametru pak zpětně získáváme nepoškozený soubor.

Teoreticky vzato by tedy bylo možné ve slackspace ukrývat před hackery také důležité vlastní informace. Taková „schovávačka“ by však byla velmi nejistá, neboť zde se mohou data snadno ztratit. Zejména v případě, kdy je soubor, který příslušnou slackspace vytvořil, odstraněn. Pokud pak totiž operační systém na jeho místo zapíše jiný soubor větší délky, budou data v původní slackspace poškozena.

Protiopatření: Jsou-li data v slackspace zašifrována, neexistuje prakticky žádná naděje, že by je bylo možné odhalit. I tak jim však stále hrozí nebezpečí výše popsaného poškození nebo přepsání. Pokud tedy hackerovi zabráníte v přístupu ke svému počítači, stávají se informace ve slackspace neškodnou datovou „vatou“.

BEZPEČNÝ ÚKRYT

Systém ukládá data po jednotkách zvaných klastry. Pokud soubor nezaplní celý klastr, zbývající neobsazenou oblast, tzv. „slackspace“, může hacker využít jako skrýš.



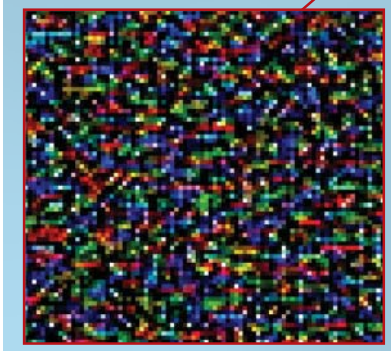
5 Digitální fotografie prozradí svého autora

Nejen kulky z pistole usvědčují pachatele. Na svého „střelce“ mohou poukázat také fotky z digitálního fotoaparátu. Neboť stejně jako drážky v hlavni zbraně zanechávají stopy na vypálené kulce, digitální fotografie s sebou nese znaky umožňující identifikovat fotopřístroj, z něhož pochází. Na vině jsou čipy CCD, obrazové senzory digitálních aparátů.

Poněvadž nejsou všechny obrazové body v senzorech identické, a mnohé jsou dokonce defektní, každý „digiťák“ zanechá ve snímku svůj „otisk prstu“. Jessica Fridrichová, profesorka na univerzitě v Binghamtonu, vyvinula program, který tento vzorek pixelové struktury prokazuje. Původně se tato vědkyně pokoušela dokazovat falšování digitálních obrazů. Její technika však dnes působí potíže například i „blogujícím“ vynašečům firemních tajemství – pokud nyní zaměstnanec nějaké firmy zveřejní na internetu fotky dosud utajovaného produktu, lze je snadno porovnat s jinými snímky, třeba z poslední letní slavnosti, uveřejněnými na soukromé domovské stránce fotografa.

Protiopatření: Postačí upravit fotografie pomocí doostřovacího filtru. Při tomto procesu se ztratí informace, které algoritmus pro identifikaci otisku potřebuje. K tomu může také dojít, jestliže internetová fotogalerie obrázky automaticky zmenšuje. Existují však už i výzkumné projekty zabývající se metodami, které by umožnily extrahovat z obrazových souborů původní informace i vzdor úpravám.

POZOR! FOTKA JE JAKO OTISK PRSTU



Silně zvětšeno: **Vědci z univerzity v Binghamtonu si vzali digitální fotografie důkladně pod lupu a objevili přitom vzory, které jsou pro každý fotoaparát jedinečné.**

6 Otevřené proxy servery mohou zmanipulovat každou webovou stránku

Kdo se chce ukrýt před spammery a podobnou sebrankou, s oblibou sahá po řešení označovaném jako proxy server. Mnohé nástroje, mezi nimi také Steganos Internet

Hrátky s proxy: **Blokovač reklam Privoxy ukazuje, co všechno je možné. Volba „Fun“ zamění v proxy serveru slovo „Microsoft“ za „MicroSuck“.**

Anonym 2006, proto na internetu hledají otevřené proxy servery. Přes ně, jak alespoň slibují, může uživatel anonymně a bezpečně surfovat. Málokdo však ví, že této metody využívají také hackeři a rovněž instalují otevřené proxy servery. Nic netušící uživatelé, kteří je použijí, slepě vbíhají do nastražené pasti. Jejím prostřednictvím se totiž hacker dozví nejen to, které stránky oběť navštívila. Hackerský proxy server dokáže zmanipulovat libovolnou webovou stránku a udělat z ní bezpečnostní riziko. Pokud hacker své peníze vydělává reklamou, má oběť ještě štěstí. Pak totiž bývají originální reklamní bannery jenom prostě vyměněny za jiné. Většinou se však touto cestou propašovávají nebezpečné skripty nebo moduly ActiveX. Tak se do kterékoli webové stránky může dostat keylogger, který každé „odposlechnuté“ heslo zašle přímo do hackerových rukou.

Sami si děláme obrázek, jak jednoduše to funguje, a instalujeme flexibilní „antireklamní“ proxy server Privoxy. Už standardní nastavení „Adventuresome“ ukazuje, co všechno je možné – například slovo „Microsoft“ vyměnit za „MicroSuck“. Ale to není všechno. Pomocí jediné vlastnoručně napsané řádky programového kódu obohacujeme každou webovou stránku o JavaScript, který nám vydá cookie webové stránky. Hacker by cookie nejspíš prostě převedl k sobě.

Protiopatření: Optimální je samozřejmě žádné cizí proxy servery nepoužívat. „Steganos Internet Anonym VPN“ se například spoléhá na vlastní servery. Ještě lepší a bezplatnou alternativou jsou v milionech případů využívané anonymizéry jako TOR nebo JAP.

7 Nové šifrování WLAN prolomeno za pár sekund

Staré šifrování bezdrátových sítí WEP rozlouskne se správnými nástroji v nejkratší době každý začátečník. Proto je nyní každý nový přístroj vybavován zlepšeným šifrováním WPA a WPA2. Že však ani tento – údajně mnohem bezpečnější – následovník algoritmu WEP hackerům neodolá, ví jen málokdo. Příčinou je, jako ostatně tak často, „lidský faktor“.

WPA totiž dovoluje jako klíče zadávat běžná slova. Uživatelé pak pro jednoduchost volí slůvka jako „Superman“, „Sparta“ nebo jméno svého partnera. Taková hesla ovšem hackeři „hrubou silou“ vypočítají skoro stejně rychle jako klíč pro WEP. Hackeři ze skupiny „Church of WiFi“ postavili dokonce speciální počítač za několik tisíc dolarů, který se nezabývá ničím jiným než prolamováním takových klíčů. Hlavní výhoda přitom spočívá v tom, že klíče se nevypočítávají pokaždé znovu, nýbrž pouze jednou, a shromažďují se v obří databance. Tak má každý hacker disponující dostatečným prostorem na pevném disku přístup k výsledkům drahého počítače louskajícího klíče WPA – aniž by sám musel investovat mnoho času a peněz do hardwaru.

TAJNÉ TRIKY POČÍTAČOVÉ POLICIE

Nejen finty hackerů se stále zlepšují, krok se snaží držet také jejich stíhatelé. „Computer Forensic“ – tak se jmenuje nová kriminalistická disciplína, která se snaží přijít na stopu „digitálním zločincům“.

Mobil v umělém rádiovém stínu

Největším problémem při domovních prohlídkách jsou nežádoucí rádiová spojení a automatizované procesy, které mohou zahladit hackerské stopy. Tak například zabavený mobilní telefon nesmí být vypnut, aby se neztratily informace z jeho pracovní paměti. Aby však nikdo nemohl do mobilu poslat „killer-SMS“, která by důležité důkazy vymazala, je nutné přístroj vložit do speciálního obalu. Je jím sáček vytvářející Faradayovu klec, která blokuje signály v obou směrech.

Data v kukuřičných lupíncích

Jiná potíž policie zní podivně, stává se však stale větším problémem. Překotný vývoj a hlavně miniaturizace přístrojů umožňuje stále lépe ukrývat informace - a dokonce celé datové nosiče. Paměťové karty Micro SD dnes už nejsou větší než desetikoruna a uskladní přitom gigabajt dat. Nelze se pak divit, že lze takovou kartu snadno schovat třeba v krabičce kukuřičných lupínků.

Informace ukryté ve fotkách

Mnohdy není k zatčení pachatele zapotřebí ani „digitální otisk prstů“. Často poskytnou dostatek důkazů i pouhá metadata, jako EXIF v digitálních fotografiích. Tam lze nalézt kromě typu fotoaparátu například i čas pořízení snímku, což může potvrdit, anebo také vyvrátit výpověď. A v budoucnu tam nejspíš budou i údaje z GPS. Sony už takové rozšíření pro svou řadu Cyber shot prodává.

Druhý život pro vymazaná data

Absolutní klasikou počítačové kriminalistiky samozřejmě je a zůstane obnova souborů. Tam, kde jsou ve filmech a v televizi disky rozebírány a informace sestavovány bit po bitu, v realitě většinou stačí jednoduchý nástroj, například PhotoRescue od firmy Datarescue. A co mnozí nevědí: Tyto nástroje rekonstruují soubory nejen na pevných discích, ale i ve flash pamětech, jako jsou karty SD, MMC nebo USB paměti.

Protiopatření: Používejte co nejkomplikovanější WPA klíče. V žádném případě slovo, které lze nalézt v lexikonu. Nejrozumnější je zvolit alespoň osm znaků dlouhou kombinaci písmen, číslic a zvláštních znaků.

8 Nebezpečné MMS infikují smartphony

Moderní mobilní telefony toho umějí čím dál tím více, a úplně nejvíc chytré jsou smartphony. Proto se tyto minipočítače také stále častěji ocitají na mušce hackerů. Otevřený operační systém jako Symbian OS nebo Windows Mobile spouští pochopitelně nejen praktické nástroje, ale také sprosté trojské koně – právě tak, jak to známe u PC. A přitom k tomu ani není třeba odněkud stahovat a instalovat programy nebo se stát obětí bezpečnostní mezery v podpoře Bluetooth. Stačí jedna infikovaná MMS. Sotva ji příjemce otevře, už má trojského koně v přístroji.

Existuje už i „proof-of-concept" bez škodlivého programového kódu. Prostřednictvím zprávy „You are owned" nám na hackerském veletrhu DefCon demonstroval technickou proveditelnost objevitel „zadních vrátek" Collin Mulliner. Momentálně to funguje jen pro Windows Mobile. Jiné operační systémy však mají – a nepochybně také budou – brzy následovat.

Protiopatření: Mnoho možností bohužel není. V každém případě by vždy měl být v mobilu nainstalován nejnovější firmware. Nedávno byla například pro mnoho telefonů k dispozici aktualizace, která uzavřela kritické bezpečnostní mezery v podpoře Bluetooth. Nejlépe je informovat se na webové stránce výrobce. Je také možné nechat si aktualizaci provést za poplatek v obchodě s mobilními telefony. Kromě toho se už pro Windows Mobile objevují také virové skenery a firewally.

Nebezpečný kufr: Tzv. „blue bag" ukrývá PC s rozhraním Bluetooth, jímž se hacker může nepozorovaně nabourat do mobilů v okolí.

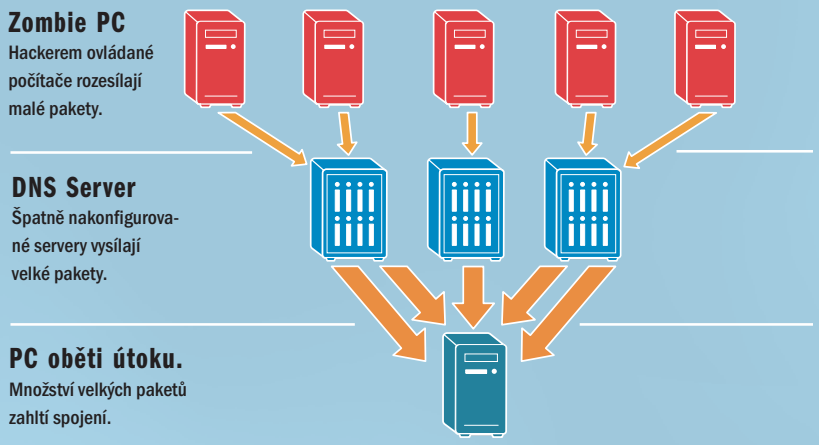
9 Odhalení anonymních surfařů

„Traffic Analysis" – tak se jmenuje nová noční můra anonymních surfařů. Až dosud byly služby jako TOR nebo JAP považovány za bezpečné a anonymní. U dvou nejoblíbenějších sítí byly pakety silně zašifrovány a rozděleny, takže jejich zpětné vysledování normálními prostředky bylo příliš náročné. Při diskusním posezení na DefCon však PGP hacker Jon Callas tuto záležitost poněkud zpochybnil. Algoritmy, které jsou toho času mimo jiné zkoumány na univerzitě v Texasu, mají jen na základě velmi skromných informací, jako je čas, časový úsek a velikost, umět určit původ paketů. Že nejde jen o fámu, dokazuje už delší dobu známý příklad: Ačkoliv síťový nástroj SSH používá velmi silné šifrování, dokázali útočníci zjistit, co uživatel zapisoval do příkazového řádku. Pouhá znalost faktu, že časová prodleva mezi písmeny „a" a „f" je delší než mezi „a" a „s", může postačit k uhádnutí celého slova. A podobně se lze dostat na kobylku i anonymizérům.

Protiopatření: Tato technika dosud nevyrostla z dětských střevíčků, příliš velké starosti si s ní tedy zatím dělat nemusíte. Hackeři, jako třeba autor TOR, kromě toho doufají, že současně s opravdovými útoky vzniknou také lepší obranné algoritmy.

JAK HACKEŘI ZAHLCUJÍ INTERNET

Hackeři bombardují DNS servery malými pakety požadavků, u nichž je podvržena adresa odesílatele. DNS servery pak bezbranné oběti odesílají jako odpovědi podstatně větší pakety, pod jejichž náporem spojení zkolabuje.



10 Doménové servery ochromují internet

Existují i bezpečnostní mezery, které nebudou zaceleny nikdy. Zde ani není důležité, kolik počítačů jde kvůli těmto chybám „do kolen". Příkladem je nejstarší internetová služba vůbec, totiž DNS (Domain Name Service). Její problém spočívá v tom, že odpovědi u ní vytvářejí větší pakety, než jaké generuje požadavek. DNS pakety nesou kromě informace, která IP adresa patří ke kterému doménovému jménu, také pole s komentářem. V něm jsou, pokud je administrátor uvede, uloženy doplňkové informace, jako je stanoviště počítače ap. Stává se tak, že mnohé doménové servery odpovídají v podobě paketů třeba až stokrát větších než původní požadavek. To by samo o sobě ještě problém nebyl. DNS však pracuje s protokolem UDP (na rozdíl od HTTP s TCP, kde každý paket musí být potvrzen). Hacker tedy může zfalšovat adresu odesílatele, aniž by to DNS server poznal.

Typický útok pak probíhá takto: Hacker rozešle prostřednictvím sítě „botů" miliony falešných požadavků různým doménovým serverům. Ty pak odpovědí relativně velkými pakety, které všechny posílají nešťastnému „odesílateli". Výsledkem je, že spojení k oběti se pod přívalem paketů zhroutí.

Protiopatření: Sama oběť takového spiknutí vlastně nemá žádnou šanci. Jediní, kdo proti tomu mohou něco podniknout, jsou provozovatelé DNS serverů. Že by však jednou byly skutečně všechny servery na internetu chráněny proti této sortě útoků, lze doufat jen stěží. ■ ■ ■